

U.S. Serial No. 09/783,112

Page 5

REMARKS

Claims 1, 10, 26 and 27 are pending.

Claims 1, 10, 26 and 27 are rejected under 35 USC 103 as being unpatentable over the Monroe et al. U.S. Patent No. 5,293,388 in view of Davis U.S. Patent No. 5,825,879 and Barnes et al. 4,172,213.

Claim 1 recites a system comprising a computer bus, a host processor connected to the computer bus, the host processor being programmed to perform error code correction, and a drive. The drive includes means for providing a block of ECC-encoded data, means for providing an encryption mask, and means for performing a bitwise XOR of the encryption mask and the block of ECC-encoded data. A product of the bitwise XOR is an encrypted block. An output of the bitwise XOR means is coupled to the computer bus.

The encrypted block can be sent to the host processor via the computer bus for error code correction. Because XOR encryption is used, the host can perform the error code correction without having to decrypt the block. The error code corrected - yet still encrypted - block can then be sent to another device, such as a DVD decoder card, for decryption.

Figures 1-3 of Monroe et al. show a computer 10 including a host processor 80; a computer bus 20 that is connected to the computer 10; and a disk 30 that is connected to the bus 20 via an adapter 40. Figure 1 also shows a peripheral 50 (e.g., a backup tape drive) that is connected to the bus 20 via an adapter 60. The adapter 60 includes an ECC co-processor 65 and ECC RAM 66. The adapter sends compressed ECC data to the peripheral 50 (col. 1, lines 55-58).

U.S. Serial No. 09/783,112

Page 6

Monroe et al. do not teach or suggest means for providing an encryption mask, and means for performing a bitwise XOR of the encryption mask and the block of ECC-encoded data. Monroe et al. do not even teach or suggest encryption of the compressed ECC block.

Moreover, in Monroe et al.'s system, the adapter does not send the compressed ECC data to the processor 80. The host computer 10 sends data to the adapter 60, and the adapter sends the compressed ECC data to the peripheral 50 (see col. 1, line 67 to col. 2, line 16). A peripheral 50 such as a backup tape driver can store the compressed ECC data.

Figure 1 of Davis shows a computer including a processor 104 and disk control subsystem 108 that are connected to a bus 128. Figure 1 also shows a video subsystem 116 connected to the bus 128. The video subsystem 116 includes a secure video content processor (SVCP) 132 for converting incoming digital content into an analog signal (see col. 2, lines 54-58)

The SVCP 132 of Figure 1 corresponds to the SCVP 200 of Figure 2. The SCVP 200 includes decryption and decompression circuitry 228 that receives encrypted video content 212 from a CD ROM 220. According to Figure 5, the SVCP 200 decrypts the video (512), processes the video data (514), re-encrypts the video data (516), and transmits the re-encrypted data to a memory unit.

Davis discloses none of the limitations of claim 1. Davis does not teach or suggest a drive including means for providing a block of ECC-encoded data, means for providing an encryption mask, and means for performing a bitwise XOR of the encryption mask and the block of ECC-encoded data, an output of the bitwise XOR means coupled to a computer bus.

U.S. Serial No. 09/783,112

Page 7

Davis is silent about ECC decoding. Encryption is performed with a public key (col. 3, lines 1-12), not XOR encryption with an encryption mask.

Barnes et al. disclose XOR encryption, but is silent about ECC coding. The office action suggests that data stored in the storage device of Figure 1 is ECC coded, and that XOR encryption is performed on the ECC coded data. However, Figure 1 suggests the opposite. Figure 1 suggests that the data stored on the data storage is ECC decoded and then outputted from the storage unit before it is XOR-encrypted.

Thus Barnes et al. does not teach or suggest a bitwise XOR of the encryption mask and a block of ECC-encoded data. Moreover, Barnes et al. do not teach or suggest the advantage of using XOR encryption on ECC encoded data. XOR encryption allows the host to perform the error code correction without having to decrypt the block. The error code corrected - yet still encrypted - block can then be sent to another device, such as a DVD decoder card, for decryption.

Thus none of the cited documents teach or suggest the system of claim 1. Accordingly, claim 1 and its dependent claim 10 should be allowable over the combination of Monroe et al., Davis and Barnes et al.

Claims 26 and 27 should be allowed for the same reasons that claim 1 should be allowed. Claim 28, which has been added to the application, should also be allowed for the same reasons.

The specification has been amended to add a patent number in the Cross Reference to Related Applications. No new subject matter has been added.

U.S. Serial No. 09/783,112

Page 8

Objections to the declaration and drawings are noted. The examiner is respectfully requested to hold these objections in abeyance until allowable subject matter is indicated.

It is respectfully submitted that the present application is in condition for allowance. Reconsideration and allowance of the present application are earnestly solicited